CLAIMS

1. A method for distributing encryption keys in WLAN, said WLAN comprising an AP and a plurality of mobile hosts storing identification information, said mobile hosts communicating with said AP through wireless channels, said AP and the external network connecting with the authentication device which authenticates said mobile hosts; said authentication device storing identification information of all mobile hosts, said method comprising the following steps:

(1) a mobile host sending an authentication request containing identification information to the authentication device for identity authentication;

(2) the authentication device authenticating the mobile host according to identification information contained in the authentication request, if the authentication fails, the authentication device sending an ACCEPT_REJECT message to the mobile host via the AP; if the authentication succeeds, the authentication device sending key-related information M1 to AP and sending an message comprising ACCESS_ACCEPT information to the mobile host via the AP; if containing key-related information M2, said message being encrypted;

(3) AP obtaining the key from the key-related information M1 sent from the authentication device, and the mobile host obtaining the key from said message sent from the authentication device via the AP.

2. A method for distributing encryption keys in WLAN according to claim 1, wherein said information M1 is the corresponding property information searched by said

authentication device according to the identification information contained in the authentication request, said AP obtains the key through generating it from said property information with a key generation algorithm; whereas said mobile host obtains the key through generating it from property information stored in itself with the same key generation algorithm after said mobile host receives said message comprising ACCESS_ACCEPT information forwarded by AP.

3. A method for distributing encryption keys in WLAN according to claim 1, wherein said information M1 is the corresponding property information searched by said authentication device according to the identification information contained in the authentication request, said AP obtains the key through generating it with a key generation algorithm; said information M2 is the key generated and encrypted by AP with said property information and then sent to said mobile host along with said ACCESS_ACCEPT message, said mobile host obtains the key through decrypting information M2 with said property information.

4. A method for distributing encryption keys in WLAN according to claim 1, wherein said information M1 is the key generated from said property information corresponding to the identification information contained in said authentication request by said authentication device with a key generation algorithm, said mobile host obtains the key through generating it from said property information stored in itself with the same key generation algorithm after receiving said ACCESS_ACCEPT message.

5. A method for distributing encryption keys in WLAN

according to claim 1, wherein said information M1 and M2 are the key generated from said property information corresponding to the identification information contained in said authentication request by said authentication device with a key generation algorithm, said information M2 is encrypted with said property information and then sent to said mobile host along with said ACCESS_ACCEPT message, said mobile host obtains the key through decrypting said information M2 with the property information stored in itself after receiving said ACCESS_ACCEPT message.

6. A method for distributing encryption keys in WLAN according to any of claim 1 to 5, wherein when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of:

(a1) said AP generating a random number and generating a new key from said random number with any key generation algorithm;

(b1) said AP adding said random number to a key update message and then sending said message to said mobile host;

(c1) when receiving said key update message, said mobile host generating a new key from said random number contained in said key update message with the same key generation algorithm as that in step (a1);

(d1) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate

the communication key has been changed; and

(e1) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

7. A method for distributing encryption keys in WLAN according to any of claim 1 to 5, wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of:

(a2) said AP generating a new key in any way and encrypting said new key with the present key;

(b2) said AP adding the encrypted key to the key update message and then sending said message to said mobile host;

(c2) when receiving said key update message, said mobile host decrypting the new key contained in said key update message with the present key so as to obtain said new key;

(d2) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and

(e2) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

8. A method for distributing encryption keys in WLAN according to any of claim 1 to 5, wherein when receiving the data packets encrypted with the key sent from said mobile host,

said AP updates the key periodically or aperiodically through the following steps of:

(a3) said Authentication device generating a random number which is used to generate a new key with the key generation algorithm, and then said authentication device sending said new key to AP, and sending said random number to said mobile host via AP;

(b3) said AP sending said key update message to said mobile host after receiving said new key;

(c3) when receiving said random number from said authentication device and said key update message from AP, said mobile host generating a new key from said random number with the same key generation algorithm as that in step (a3);

(d3) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and

(e3) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

9. A method for distributing encryption keys in WLAN according to any of claim 1 to 5, wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically through the following steps of:

(a4) said AP generating a new key in any way and encrypting

said new key with the present key, then sending said new key to said AP, whereas sending the encrypted new key to said mobile host via said AP;

(b4) after receiving said new key, said AP sending a key update message to said mobile host;

(c4) when receiving the encrypted key from said authentication device and said key update message from said AP, said mobile host decrypting the encrypted key with the present key to obtain a new key;

(d4) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed; and

(e4) when receiving the data packets from said mobile host, said AP determines whether to change the key according to value of said encryption identifier.

10. A method for distributing encryption keys in WLAN according to any of claim 1 to 5, wherein said authentication device is an authentication server installed in said external network.

11. A method for distributing encryption keys in WLAN according to claim 6, wherein said authentication device is an authentication server installed in said external network.

12. A method for distributing encryption keys in WLAN according to claim 7, wherein said authentication device is an authentication server installed in said external network.

13. A method for distributing encryption keys in WLAN

according to claim 8, wherein said authentication device is an authentication server installed in said external network.

14. A method for distributing encryption keys in WLAN according to claim 9, wherein said authentication device is an authentication server installed in said external network.

15. A method for distributing encryption keys in WLAN according to any of claim 1 to 5, wherein said authentication device is a wireless gateway that connects said AP with said external network.

16. A method for distributing encryption keys in WLAN according to claim 6, wherein said authentication device is a wireless gateway that connects said AP with said external network.

17. A method for distributing encryption keys in WLAN according to claim 7, wherein said authentication device is a wireless gateway that connects said AP with said external network.

18. A method for distributing encryption keys in WLAN according to claim 8, wherein said authentication device is a wireless gateway that connects said AP with said external network.

19. A method for distributing encryption keys in WLAN according to claim 9, wherein said authentication device is a wireless gateway that connects said AP with said external network.

20. A method for distributing encryption keys in WLAN according to any of claim 1 to 5, wherein said authentication device includes said wireless gateway and said authentication server installed in external network.

21. A method for distributing encryption keys in WLAN according to claim 6, wherein said authentication device includes said wireless gateway and said authentication server installed in external network.

22. A method for distributing encryption keys in WLAN according to claim 7, wherein said authentication device includes said wireless gateway and said authentication server installed in external network.

23. A method for distributing encryption keys in WLAN according to claim 8, wherein said authentication device includes said wireless gateway and said authentication server installed in external network.

24. A method for distributing encryption keys in WLAN according to claim 9, wherein said authentication device includes said wireless gateway and said authentication server installed in external network.